

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

# UK Patent Application (19) GB (11) 2 371 888 (13) A

(43) Date of A Publication 07.08.2002

(21) Application No 0102428.0	(51) INT CL <sup>7</sup> G06F 1/00 12/14
(22) Date of Filing 31.01.2001	(52) UK CL (Edition T ) G4A AAP
(71) Applicant(s) Hewlett Packard Company (Incorporated in USA - Delaware) 3000 Hanover Street, Palo Alto, California 94304, United States of America	(56) Documents Cited EP 1091275 A EP 0935182 A EP 0929023 A WO 1998/007254 A
(72) Inventor(s) Luca Chiarabini Anthony J Wiley	(58) Field of Search UK CL (Edition S ) G4A AAP INT CL <sup>7</sup> G06F 1/00 3/12 12/14 Online: WPI, EPDOC, JAPIO, INSPEC
(74) Agent and/or Address for Service Franks & Co 9 President Buildings, Savile Street East, SHEFFIELD, S4 7UQ, United Kingdom	

(54) Abstract Title  
A printer device capable of decrypting digital document files and method of securely communicating electronic files over a network

(57) A printer device comprises a data input device for receiving encrypted digital document files, a decryption algorithm for decrypting document files, a controller for controlling the printing of an image of data contained in the received file and a printer mechanism for printing a physical copy of the file. The controller operates the printing of the physical copy and after printing, deletes the electronic document file from the memory. Also disclosed is a computer entity comprising a data processor, memory, encryption algorithm, device selector, file selector and a stored list of set authorised recipient devices identified by unique identifier data inaccessibly embedded. The computer selects document files, selects printers, encrypts the files and addresses them to the selected uniquely identified devices. There is a system comprising a computer and recipient printer device, and a computer entity with an attached printer device.

Also disclosed is a method of secure communication over a network by encrypting a document file, specifying a printer, attaching unique device identifier data, sending the file, receiving it, decrypting it, reading the identifier data, comparing it with a stored identifier data in the recipient device and if these match, printing the file.

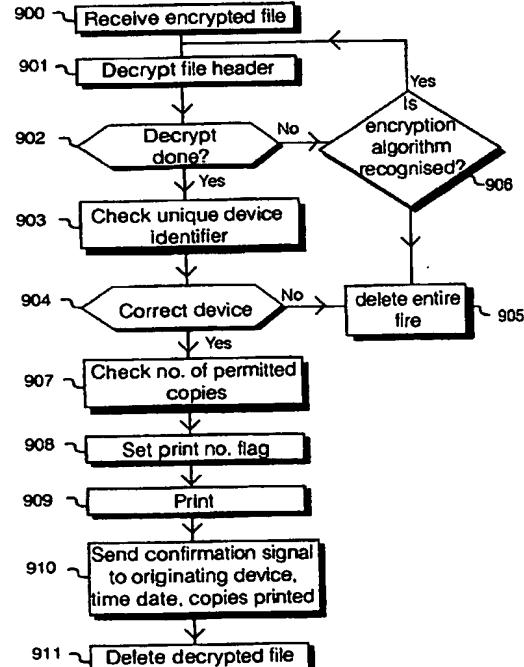


Fig. 9

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

GB 2 371 888 A

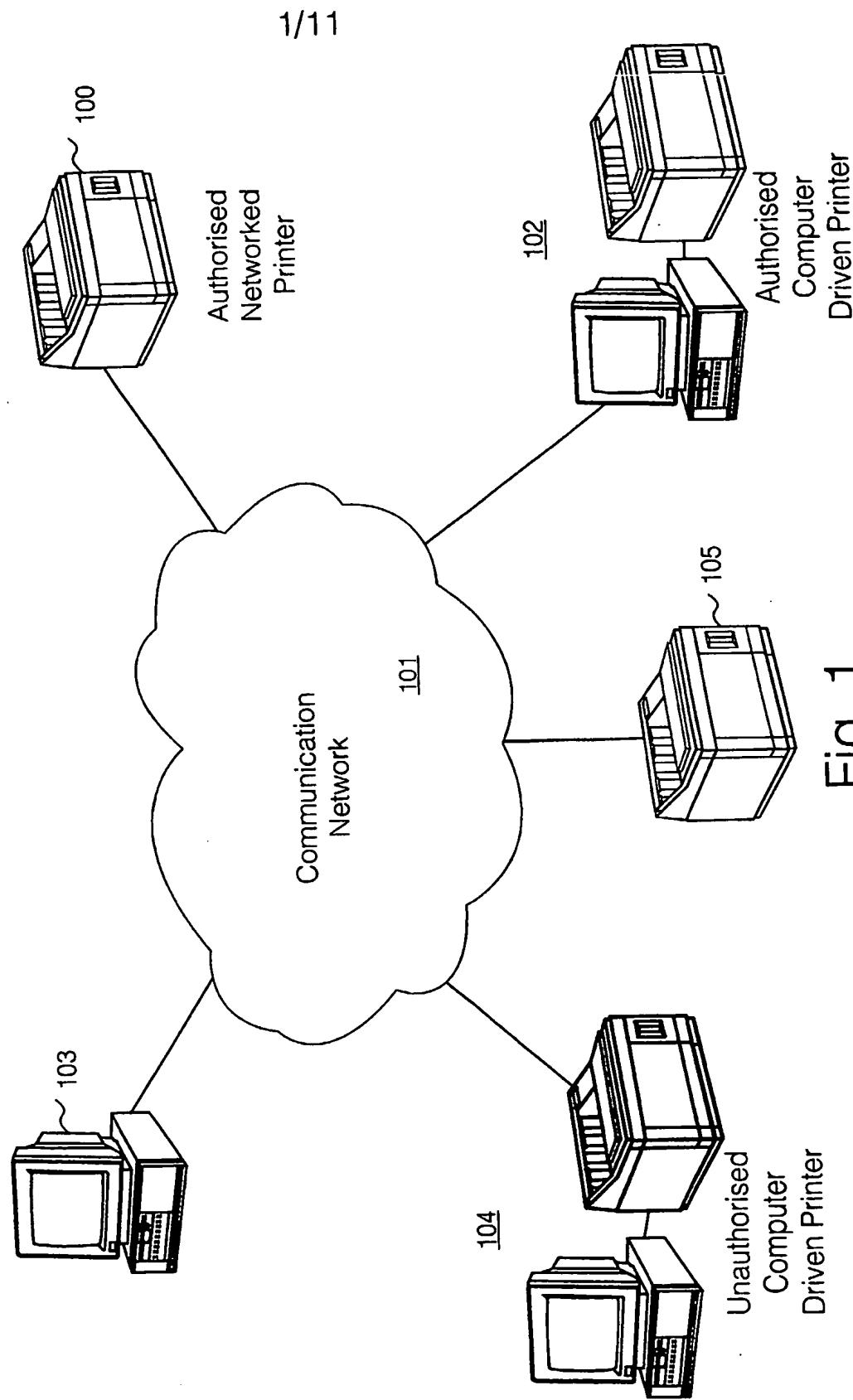


Fig. 1

2/11

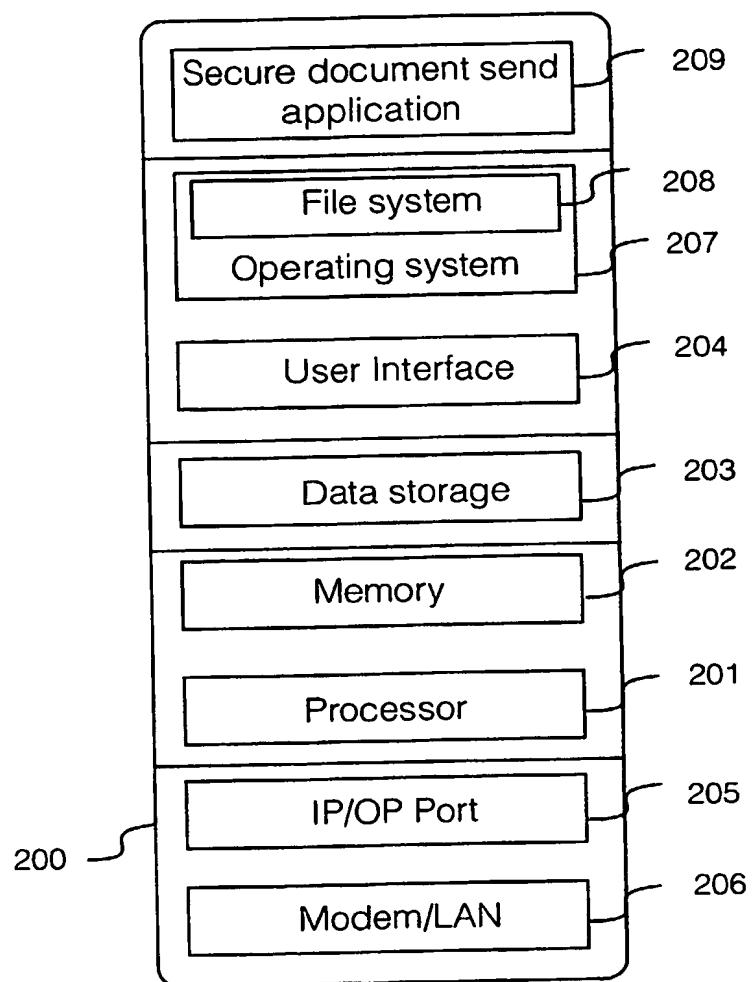


Fig. 2

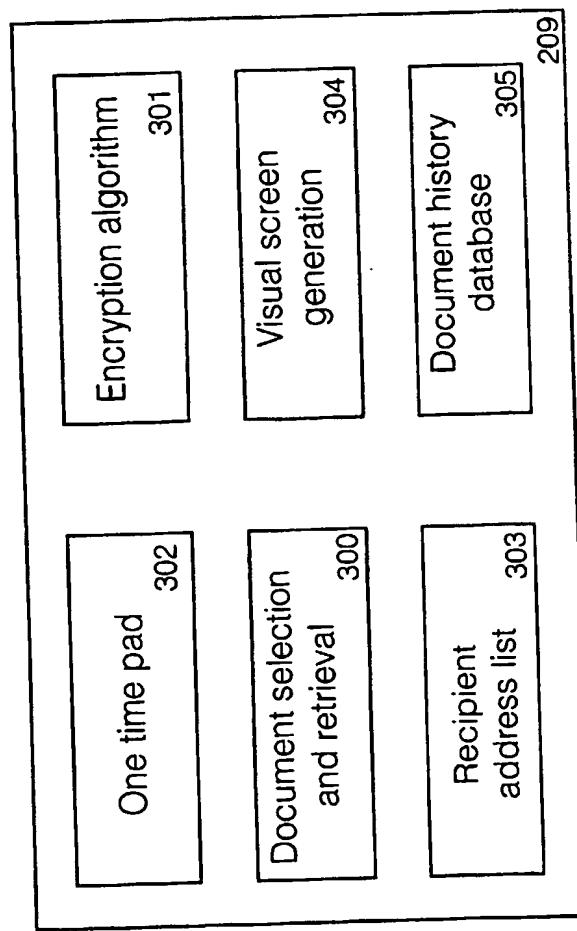


Fig. 3

4/11

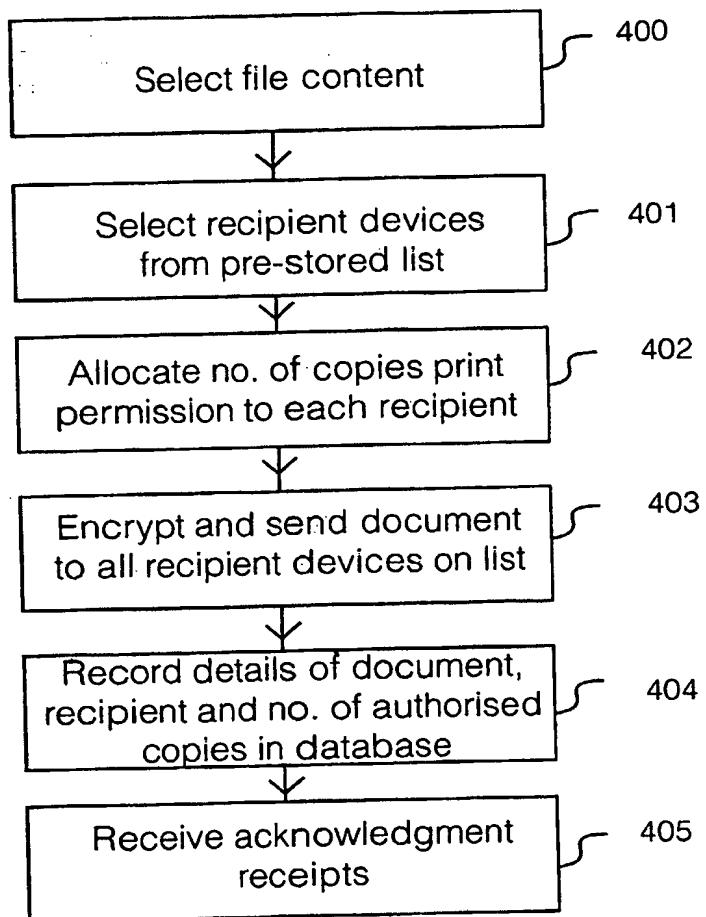


Fig. 4

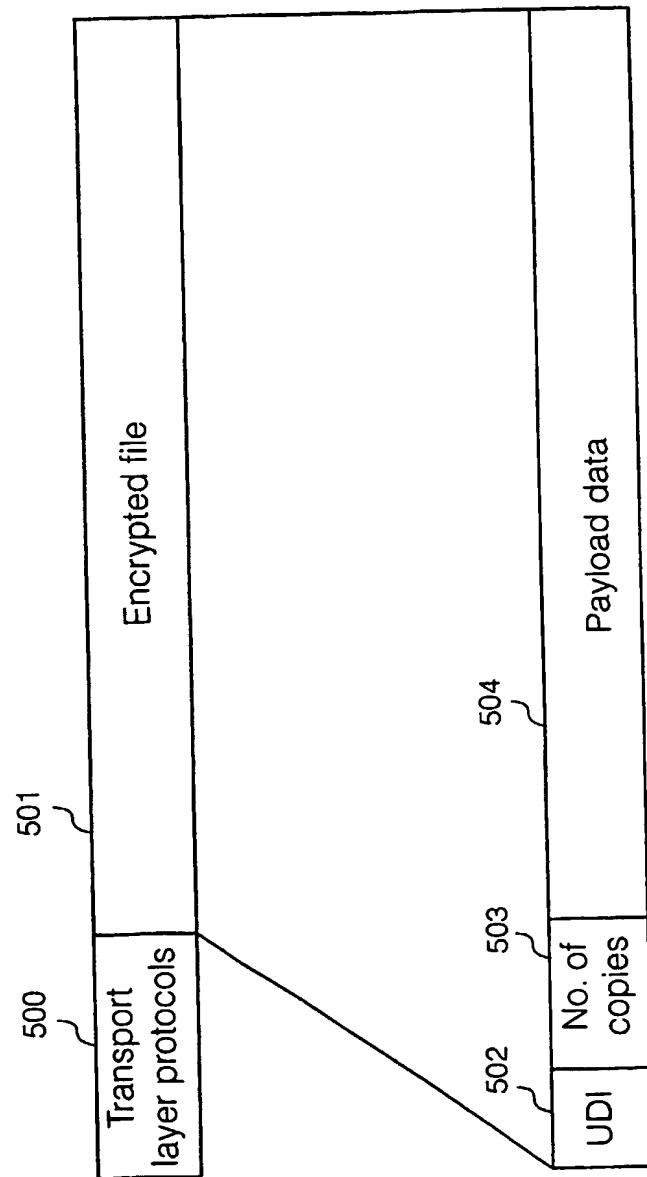


Fig. 5

30.4.02

6/11

Distribution list				
Document name:	Copies	Acknowledge		
Document name: company report.doc	Copies	Acknowledge		
Applianct: Word 2000	1	01.01.2001	603	
R1 address R1 OTK 1	1	21.50		
R2 address R2 OTK 3	1	01.01.2001	21.50.30	
R3 address R3 OTK 5	1	01.01.2001	21.52	
R4 address R4 OTK 17	2	01.01.2001	21.51	
600	601	602		

Fig. 6

30 44 02

7/11

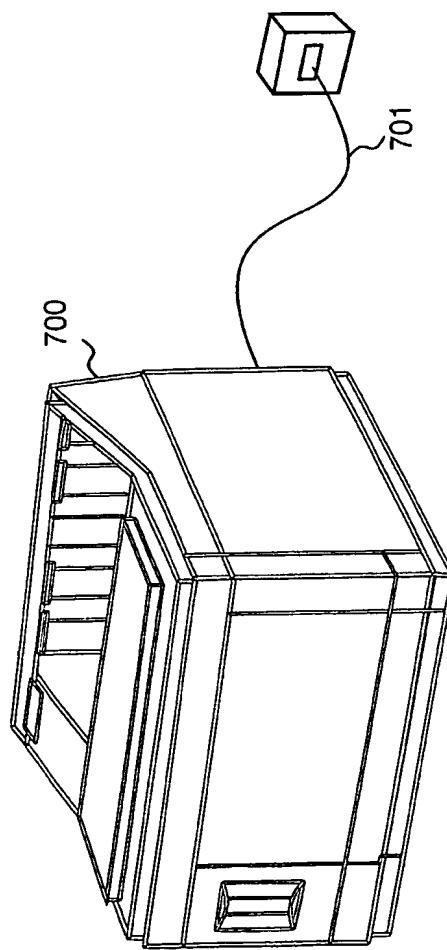


Fig. 7

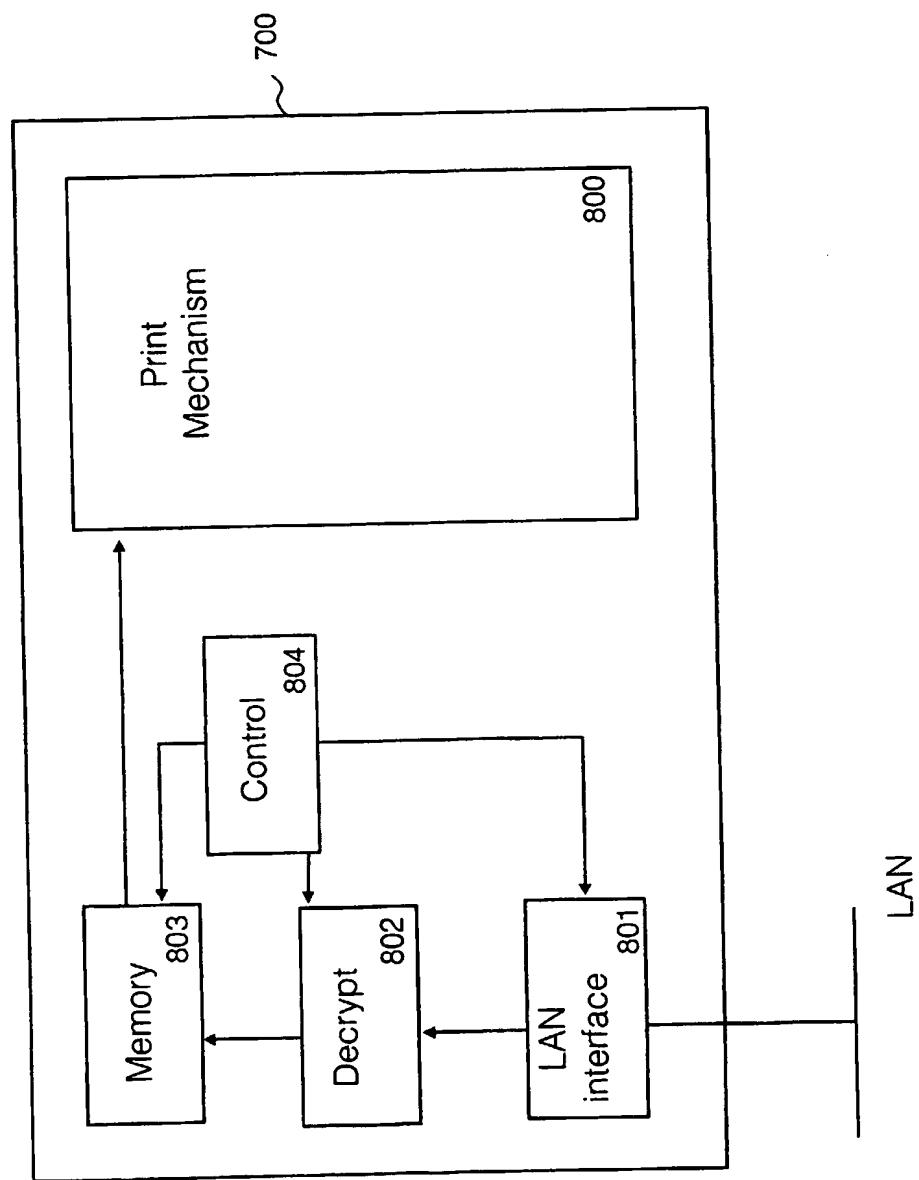


Fig. 8

9/11

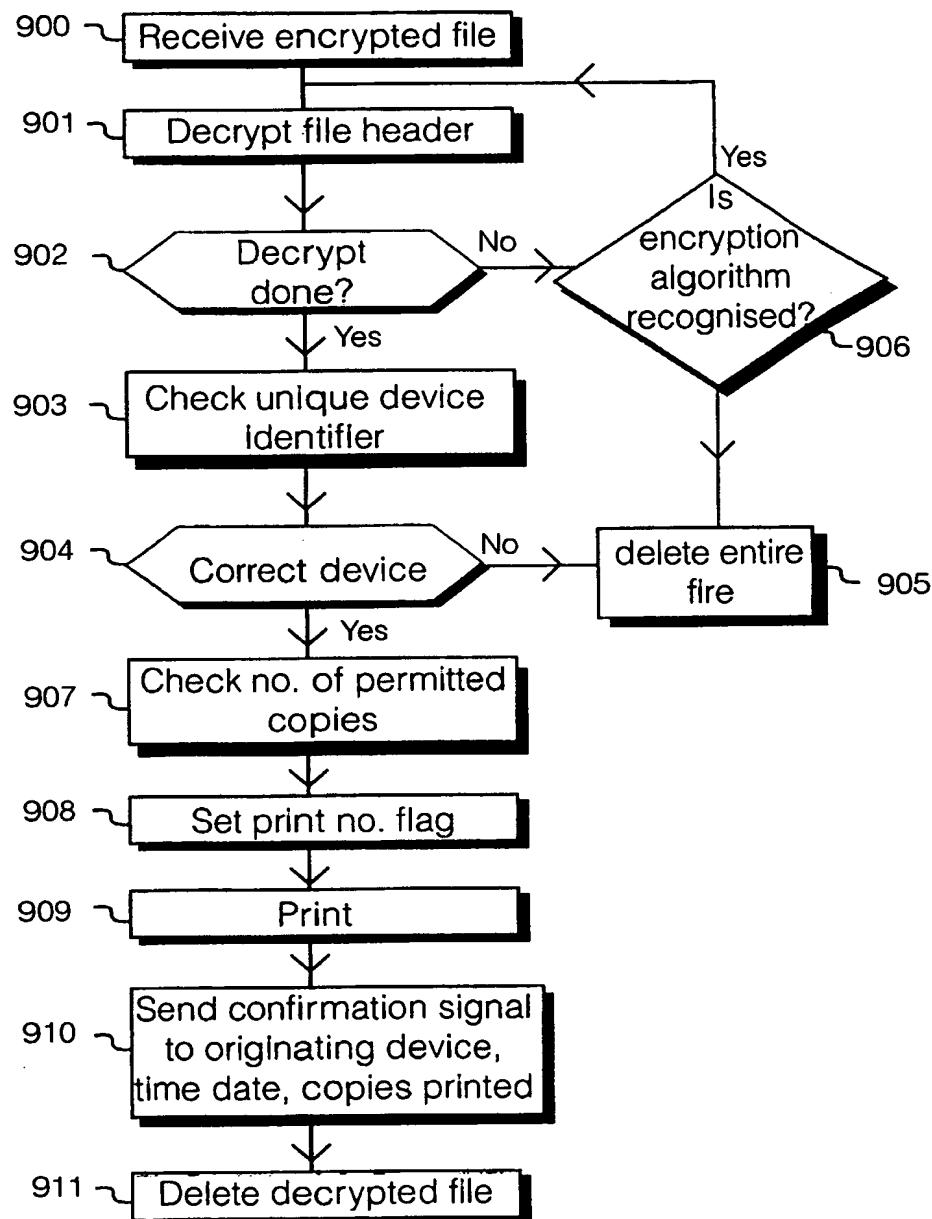


Fig. 9

10/11

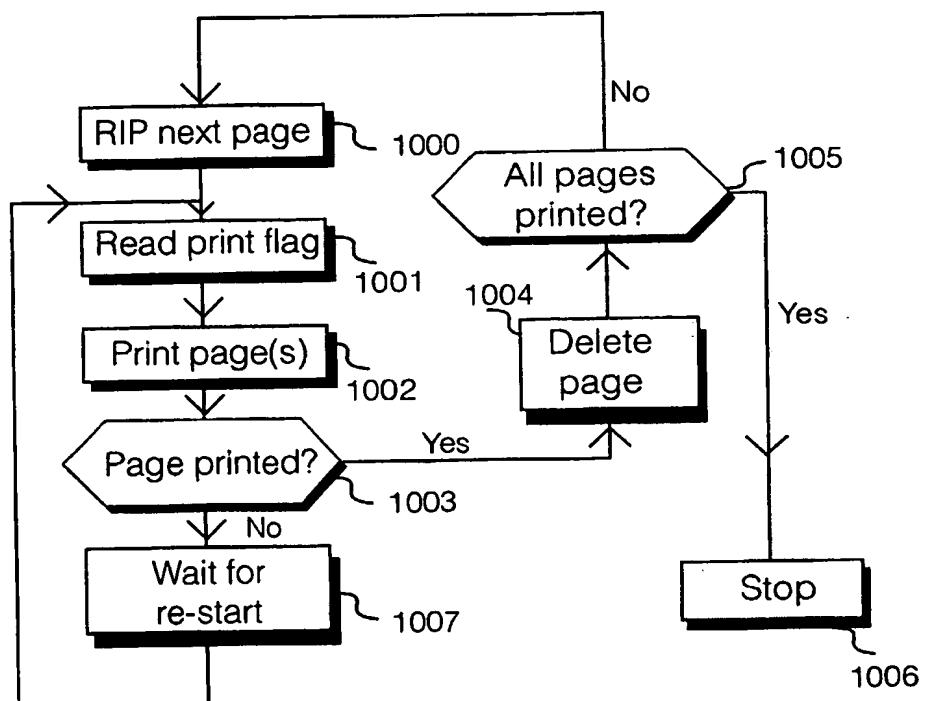


Fig. 10

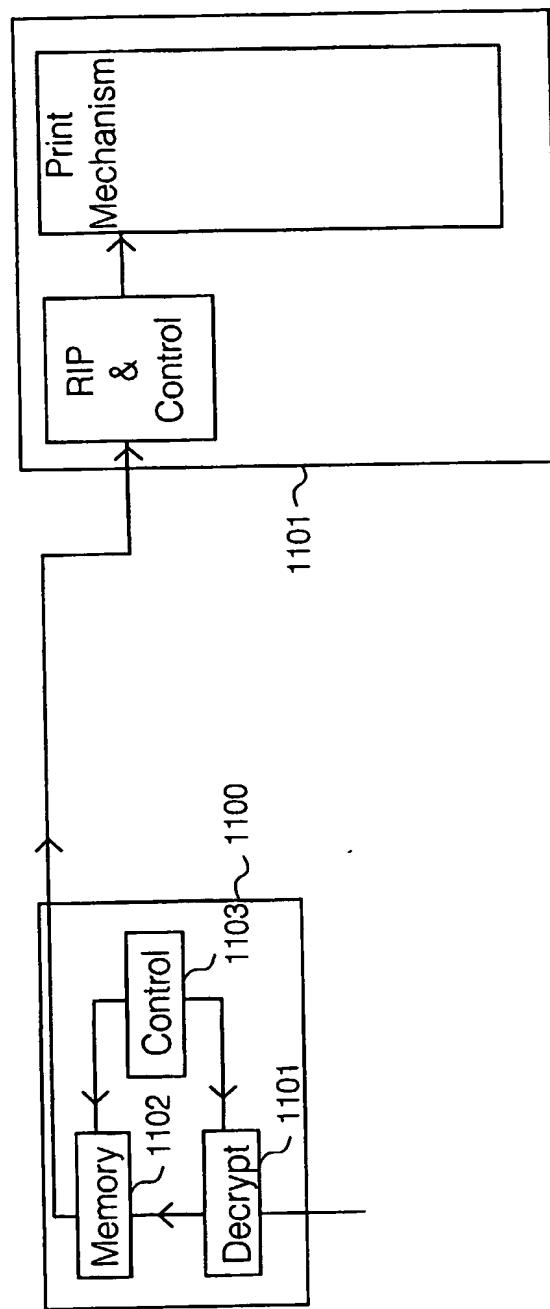


Fig. 11

**A MECHANISM FOR CONTROLLING IF/WHEN MATERIAL CAN BE  
PRINTED ON A SPECIFIC PRINTER**

**Field of the Invention**

5       The present invention relates to the field of document printing, and particularly although not exclusively, to secure printing of documents.

**Background to the Invention**

10      Conventional solutions for secure printing attach printing rights to an individual person. Typically, a person sending a secure text and/or image file, may encrypt that file, send it over a network to a recipient, and the recipient, on receiving the file, decrypts the file using a known encryption mechanism, on a personal computer (PC) or other equivalent computer entity. Having decrypted the file, the recipient can send the file to print, load the file onto a data carrier such as a floppy disk, writable CD ROM, digital data storage (DDS) format device or similar. Prior art systems have the characteristic that firstly, once decrypted, there is no limitation on the number of prints which can be made from a received file. Secondly, receipt of the document is location independent. Provided the correct decryption software is loaded into a computer entity, there is no restriction 15     on where the document can be decoded or on which individual computer entity, or printer device printing of a document can take place. Thirdly, the ability to decrypt data follows possession of a decryption key and decryption software, and a person having that key and software has potentially no physically enforceable 20     restrictions on use of the document once decrypted.

25      In commercial or government organisations, different types of information are accorded different levels of security. For example, a typical four level security system may comprise:

30      •     Level zero – documents freely available to anyone inside or outside the organisation, publicly available material.

- Level one – documents which are restricted for employees or personnel within the organisation, and which are not to be released outside the organisation.

5

- Level two – documents which are of a company confidential nature, such as technical reports, project specifications, and documents for which there would be commercial or other disadvantage in allowing to leak outside the organisation

10

- Level three – documents having restricted access to named individuals, for example take over/merger plans, personnel files, details of individuals salaries, business plans, financially sensitive data such as company financial accounts before publication, and defense or governmental classified information.

15 For higher security level information, individual paper documents may be individually numbered, and named individuals authorised to read the documents listed within the documents. Documents may be subject to restrictions, such as a bar on photocopying the documents, and restriction on the number of physical copies in circulation.

20 Electronic storage of such documents may also be restricted to machines which can be physically locked away.

25

With prior art secure electronic document solutions using computers, a recipient is allowed access to an electronic version of a file, which can be loaded onto a data carrier. The underlying assumption is that a person authorised at a particular security level has access to information in electronic storables format.

30 However, whilst physical paper documents containing information are readily physically identifiable and can be checked by security personnel on leaving a

building, electronic data can be easily passed out of an organisations premises and computer networks by electronic means, and in large quantities, without trace.

5        Although paper based information is not entirely secure, and is capable of being photocopied or sent by facsimile, it requires more time and effort to photocopy documents, or send them by facsimile, than it does to send documents electronically. The speed of sending electronic documents, and the 10 large data volumes which can be sent without trace, make electronic storage of documents inherently less traceable and less secure, than the same information stored in paper format.

**Summary of the Invention**

15      Specific implementations according to the present invention associate rights to a digital object for example a document file, such that it is only possible to print the object on a pre-defined set of devices. Ownership and access of the devices is restricted, and the devices may be physically placed in secure areas.

20      By associating a restrictive set of rights to an object which explicitly identifies which devices the object may be printed on, a level of physical security can be applied to the printing of electronic data files. Files may be sent in encrypted format to a secure print room, which may ensure that unauthorized access to the encrypted file would not result in it being printed elsewhere.

25      An authorised device is able to identify whether any restrictive rights are applicable to an object being presented for printing, and depending upon the restrictions, either delete the object, or print it.

30      Specific implementations explicitly specify which devices may be used to print a particular file, thereby providing an extra level of physical security. Further, limits on a number of copies of a file which may be printed may be enforced.

According to a first aspect of the present invention there is provided a network connectable printer device comprising:

- 5 a data input device for receiving an encrypted digital document file;
- 10 a decryption algorithm for decrypting said received document file;
- 15 a controller for controlling printing of an image of data contained in said received document file; and
- 20 a printer mechanism for printing a physical copy of said document file,  
wherein said controller operates to control printing of said physical copy,  
and after printing of said physical copy, delete said electronic document file from  
25 said memory.

According to a second aspect of the present invention there is provided a printer device comprising:

- 20 a data input device for receiving an encrypted digital document file;
- 25 a decryption algorithm for decrypting said received document file;
- 30 a controller for controlling printing of an image of data contained in said received documents file; and
- 35 a printer mechanism for printing a physical copy of said document file,  
wherein said controller operates to check a unique device identification data  
contained in said document file with a stored unique device identification data of  
said printer device, and provided a successful match is found, print said physical  
copy of said document file.

According to a third aspect of the present invention there is provided a computer entity configured for sending secure encrypted document files, said computer entity comprising:

- 5        a data processor;
- a memory;
- an encryption algorithm capable of encrypting a document file;
- 10       a device selector for selecting a said uniquely identifiable recipient device;
- a file selector for selecting a document file;
- 15       a stored list of a set of authorised recipient devices, each said recipient device identified by a unique device identifier data inaccessibly embedded within said computer entity;
- wherein said computer entity operates to:
- 20       select at least one document file;
- select at least one device of said set of uniquely identified recipient devices to send said document to;
- 25       encrypt said document files; and
- address said at least one document file to said selected uniquely identified device(s).

According to a fourth aspect of the present invention there is provided a distributed secure document printing system, said system comprising:

- 5 at least one sending computer entity, capable of sending an encrypted electronic document file, said document file having an encrypted data content, and a unique device identifier data identifying a recipient device to which said document file is sent: and
- 10 at least one recipient printer device, said recipient printer device capable of receiving said encrypted document file, establishing that said document file is intended for said recipient device, decrypting and printing said document file, and deleting said electronic document file after printing a physical copy of a document from said document file.

- 15 According to fifth aspect of the present invention there is provided a method of securely communicating an electronic document file over a network, said method comprising the steps of:

- 20 encrypting said document file;
- specifying a recipient device for sending said document file to, said recipient device being uniquely identifiable by a unique device identifier data;
- 25 attaching said unique identifier data to said document file;
- sending said document file in encrypted format to said intended recipient device;
- 30 receiving said transmitted document file and decrypting said document file;
- reading said unique device identifier data;

if said unique device identifier data corresponds to a unique device identifier data of said recipient device, printing a physical copy of said document files.

According to a sixth aspect of the present invention there is provided a  
5 method of secure printing of a received document file, said method comprising  
the steps of:

- receiving said document file in encrypted format;
- 10 decrypting said document file;
- reading a unique device identifier data identifying a recipient device for  
which said document file is intended;
- 15 comparing said unique device identifier data with a locally stored device  
identifier data;
- if said received unique device identifier data corresponds with said locally  
stored device identifier data, printing a physical copy of said document file.
- 20 According to a seventh aspect of the present invention there is provided a  
method of sending a document file for printing by a specified authorised  
recipient printing device, said method comprising the steps of:
- 25 selecting a content of said document file;
- encrypting said content;
- attaching a unique device identifier data, identifying a recipient device to  
30 which said document file is to be sent; and
- sending said document file to said recipient device.

According to an eighth aspect of the present invention there is provided a computer entity comprising a data processor, a data storage device, a printer port, and having an attached printer device, said computer entity comprising:

5

a module for decrypting an encrypted document file;

10 a unique device identifier to identify said computer entity into a uniquely;

15 wherein said computer entity operates to:

receive a document file in encrypted format;

20 decrypt said document;

25

extract a unique device identifier data from said document and compare said extracted unique identifier data with said unique device identifier of said computer entity;

25 if a match is found between said received unique device identifier data and said unique identifier of said computer entity, send a said document file for print by said printer device; and

30 after sending said document to said printer device, delete said document file.

#### **Brief Description of the Drawings**

For a better understanding of the invention and to show how the same may be carried into effect, there will now be described by way of example only, specific embodiments, methods and processes according to the present invention with reference to the accompanying drawings in which:

Fig. 1 illustrates schematically a secure document printing system for securely printing documents over an open access network;

5 Fig. 2 illustrates schematically components of a sending computer entity for sending a secure document over said network;

Fig. 3 illustrates schematically components of an application of said sending computer entity, for formatting a document file for sending over said network, and for storing a document history data;

10 Fig. 4 illustrates schematically process steps carried out by the secure sending computer entity of Fig. 2;

15 Fig. 5 illustrates schematically a document file format of a secure document file sent over said network;

Fig. 6 illustrates schematically a visual display of a distribution list and history of documents sent over said network, displayed by said send computer entity;

20 Fig. 7 illustrates in perspective view a network attached secure printer device for securely printing document files received over said network;

25 Fig. 8 illustrates schematically internal components of said secure network attached printing device of Fig. 7;

Fig. 9 illustrates schematically process steps carried out by said secure printer device of Fig. 7 for securely printing a physical copy of said document files;

30 Fig. 10 illustrates schematically further process steps carried out by said secure printing device for printing physical copies of said document file; and

Fig. 11 illustrates schematically components of an application module installed in a computer entity with printer according to a further specific embodiment of the present invention.

5

**Detailed Description of the Best Mode for Carrying Out the Invention**

There will now be described by way of example the best mode contemplated by the inventors for carrying out the invention. In the following description numerous specific details are set forth in order to provide a thorough 10 understanding of the present invention. It will be apparent however, to one skilled in the art, that the present invention may be practiced without limitation to these specific details. In other instances, well known methods and structures have not been described in detail so as not to unnecessarily obscure the present invention.

15

Referring to Fig. 1 herein, there is illustrated schematically components in a secure printing system according to a specific implementation of the present invention. The system comprises one or more network attached secure printer devices 100 attached to a communications network 101, for example the internet, or a local area network; one or more secure receiving devices 102, each comprising a computer and printer device; and one or more secure data sending devices 103. In the network environment, there may be also attached a plurality 20 of non-secure computer devices 104 having printer capabilities, and one or more non-secure network attached printer devices 105.

25

Secure data sending device 103 sends an encrypted document file over the communications network 101, for example the internet, to a designated authorised recipient device, 100 or 102. On receiving the encrypted document file, the authorised recipient device decrypts the document file, by a known decryption mechanism, and prints out an authorised number of copies of a 30 document, which are specified in the document file sent over the communications network. Since the document file is encrypted, if the file becomes misappropriated or sent to a non authorised computer by mistake, the encryption

protects the data contained within the file. The one or plurality of authorised recipient devices are pre-registered with the secure data sending device 103, preferably at the point of manufacture, with data identifying each of the authorised recipient devices being embedded in the inaccessible software and/or hardware of the secure sending device 103. Similarly, data identifying the secure sending device 103 may be embedded in inaccessible hardware and/or software of each authorised recipient device 100, 102 at manufacture, so that the secure data sending device 103 and one or a plurality of authorised recipient devices are registered with each other by data installed into the inaccessible internal components of those devices at the point of manufacture. Therefore, a degree of trust in the secure data sending device and the recipient device(s) is given to those devices, by virtue of a purchaser or user of the system having trust in the company who manufactures the secure data sending device and recipient devices.

Whilst in the best mode implementation, document files are transferred over into an intermediate network between ascending computer entity and a recipient printer device, in other embodiments, the document file may be loaded onto an intermediate device having data storage capability, for example a mobile phone, or palm held computer entity, or lap top computer. The recipient printer device need not be network attached, but could receive a document file over an infra-red communications link, from such an intermediate device, storing the document file.

Document file transmission may be by any suitable method, for transfer into the recipient printer device. The document file may be introduced to the recipient printer device by means of a floppy disk, CD ROM, by presenting the printer device with an infra-red signal from a hand held portable data storage device, e.g. mobile phone, palm top computer entity, or lap top computer entity having infra-red transmission capability.

Referring to Fig. 2 herein, there is illustrated schematically components of a computer entity adapted to send secure documentation to one or a plurality of secure printing devices.

5        The sending computer entity 200 comprises known components including a processor 201 with associated memory 202; data storage 203, for example a hard disk drive or the like; a user interface 204, including a visual display unit, keyboard, and pointing device eg mouse or trackball device; a plurality of input/output ports 205; a modem and local area network connection 206; an  
10      10 operating system 207 having a known file system 208; and a secure document sending application, 209 according to a specific implementation of the present invention. The secure document sending application 209 presents a user interface in the form of a visual display on the video monitor, by which a user can select documents from the file system of the operating system, encrypt those  
15      15 documents, and send them to designated secure destination devices, which are pre-registered with the sending computer entity.

Referring to Fig. 3 herein, there is illustrated schematically modules of the secure document send application 209. The application comprises a document  
20      20 selection and retrieval module 300, capable of interfacing with the file system of the operating system for the retrieval and selection of individual files, typically of text and/or image data; an encryption algorithm 301 of prior art type, for example the known DES, 3DES, RC5, CAST, IDEA, or Blowfish algorithms; optionally, a one-time pad module, containing a set of one-time pad encryption keys; a  
25      25 recipient address list 303 listing electronic addresses of a plurality of pre-registered receiving devices, e.g. network attached printers; a visual screen generation module 304 for generating a visual user interface allowing selection, encryption and sending of documents to the recipient devices; and a document history database 305 listing a history of send events of documents detailing which  
30      30 documents have been sent, the destinations and number of copies sent.

Referring to Fig. 4 herein, there is illustrated schematically process steps implemented by the send computer entity 200 for sending secure documents across the network to specified recipient devices. In step 400, a user selects a file content using the user interface generated by the secure document application 209. Files may be displayed in a format similar to Windows Explorer ®, and files may be identified by drag and drop menus. In step 401 a user selects individual recipient devices from a drop-down menu of devices generated from one of the pre-stored recipient address lists 303. Each individual pre-registered device is listed, and the user may assign an individual document to an individual recipient device. In step 402, the user allocates a quantity print permission for each selected document to each authorised recipient device which the user has selected. Upon a screen, for each selected recipient device, the user may input a number data specifying a number of copies for which permission to print is to be granted. In step 403, having selected the recipient devices, selected the document to send, and allocated quantity permissions to each individual recipient device, the user activates sending of the document to all recipient devices. The document is encrypted by the encryption module 301, and sent across the network via the input/output ports 205 and modem and LAN connection 206. Transport of the encrypted document across the communications network is by conventional manner, and conventional transport protocols, for examples TCP/IP are applied. In step 404, the algorithm records the details of the documents, recipient device addresses and number of authorized copies in the history database 305 which can be accessed at any time by the user to trace where particular documents have been sent and to provide accountability of document transmission at the send computer entity. In step 405, optionally, the send computer entity may receive acknowledgments from each of the specified secure recipient printer devices, acknowledging from each of those devices that the encrypted electronic document has been received. Acknowledgement data recording time and date at which each individual recipient printer device received the document may be stored in the document history database.

Referring to Fig. 5 herein, there is illustrated schematically an encrypted file as sent by the sending computer entity. The file comprises known transport layer protocol layers, for example ATM packet headers, TCP/IP protocol headers, or the like, followed by an encrypted file content 501. The complete file, may be

5 packetized according to known transport protocols, into a plurality of packets or cells and sent as a series of individual packetized transmissions over the communications network as is known in the art. Within the encrypted portion of the file, there is included a unique device identifier data 502, a quantity print permission data 503, allowing permission for printing of a specified number of

10 copies; and a payload data 504 being the actual data for containing the information to be printed in hard copy at the recipient device, typically including text and/or image data.

15 Referring to Fig. 6 herein, there is illustrated schematically a visual display generated at the sending computer entity 200, listing distribution of a particular document. The display is generated from data stored in the document history database 305 and may include an electronic address identifier data 600 identifying a unique electronic address for each of a plurality of recipient devices;

20 data describing an encryption method used, for example a one time key or other known encryption method; a number of copies for which print permission has been given, and an acknowledgement time and date data 603 describing an acknowledgement data received from a recipient print device; a document identification data 604 identifying the documents sent; and optionally, an application data 605 identifying an application package, in which the document is

25 generated.

Referring to Fig. 7 herein, there is illustrated schematically in perspective view, a secure network attached printing device 700. The secure network attached printing device attaches directly to a network connection 701, eg a CAT5 internal wiring system in a building. The secure printer has its own network address, and receives an encrypted file. The printer decrypts the file using a

known encryption scheme, and prints out a specified number of prints of the file authorised to be printed on that device. After the file has printed, the electronic version of the file received by the printer is deleted from the printer's memory. Deletion of electronic data can be implemented by decrypting an electronic page after each physical page is printed, or by deleting the entire file after the entire file 5 has been printed in hard copy.

Referring to Fig. 8 herein, there is illustrated schematically components of the secure network attached printer device 700 of Fig. 7 herein. The printer device 10 comprises a print mechanism 800 as is known in the art including a physical transport mechanism for transporting print media, a print head, ink cartridge and control electronics; a network interface 801 e.g. a local area network interface, or a web interface; a decryption module 802 containing a decryption algorithm; a local memory area 803 for storing image data; and a control mechanism 804 for 15 controlling the processing of a data file, received over the network interface 801.

Referring to Fig. 9 herein, there is illustrated schematically process steps carried out at a secure printer device 700 for decrypting and printing a specified number of copies of a received document. In step 900, the printer device 20 receives the encrypted file in known manner. In step 901, the decryption algorithm 802 proceeds to decrypt the file using known decryption techniques. In step 902 the printer device checks a unique device identifier data 502 contained in the decrypted data file, and checks in step 903 whether that unique device identifier corresponds to the device itself. If the unique device identifier is not 25 recognized as being the devices own device identifier data, then the printer deletes the entire file from its memory.

In step 902, if decryption is determined to have been unsuccessful, then in 30 step 906, the algorithm checks whether the encryption algorithm used is of a type recognizable by the printer device. If not, then in step 905 the printer device deletes the entire file from its memory.

in step 907, the printer device checks the permitted print copy number field 503 and sets a print number flag in step 908, which determines how many copies of the file the printer will print. In step 909, the printer proceeds to print the specified number of permitted copies of the file in hard copy. In step 910, the 5 recipient printer device may send a confirmation signal back to the sending computer entity, including a time data, date data, and a number of copies printed, confirming that the printer has printed a specified number of copies at a specified time and date.

10 Referring to Fig. 10 herein, there is illustrated schematically process steps carried out by the secure printer device for printing the decrypted document. In step 1000, a page of the document is raster image processed to obtain image data in a format suitable for reading by the print mechanism 800 of the device. In step 1001, the print flag is read, and in step 1002, the print mechanism proceeds, 15 under control of the control module 804, to print the permitted copies of the page, specified by the number contained in the print flag, which is initially set at the number of authorised copies read from the quantity print data 503, and is decremented for a page each time a copy of that page is printed.

20 In step 1003, when all permitted copies of the page are printed. The page data is deleted from the memory in step 1004, and the decrypted data for the next page is raster image processed in step 1000. These steps repeat until all pages of the document have been printed in step 1005, in which case the process stops in step 1006. If at any time printing is interrupted, for example 25 because print media such as paper or ink run out, or if there is a fault, then the printer waits for a restart signal from the prior art known restart mechanisms within the printer.

30 Referring to Fig. 11 herein, there is illustrated schematically an applications program 1100 which may be installed in a conventional computer entity and conventional printer device 102 as illustrated in Fig. 1, to convert that conventional computer entity and printer device combination into an authorised

recipient device. The application 1100 comprises a decryption algorithm 1101; a control module 1102 for controlling part of the memory of the computer entity for storing of decrypted image data prior to sending to the printer; and a control module 1103.

5

Similarly as described herein before, the application operates to receive an encrypted document file, containing a unique recipient device identifier data, decrypt that document file, check that a unique device identifier data contained within the received document file matches the stored unique device identifier data embedded within the application itself, and provided the unique device identifier data received in the document file matches that embedded in the application, then to print the individual pages of image data in the document file one at a time, or the whole document at once, then deleting the electronic form of the document file from the computer entity once printing has taken place.

15

Printing may take place one page at a time, with deletion of the electronic form of the document file occurring for each page, after that page is physically rastered and printed, or alternatively the whole document file may be printed at once, and the electronic form of the document file deleted from the recipient 20 computer entity after physical printing of the whole document has been made.

25

In the embodiment shown in Fig. 11, because a conventional computer entity and conventional printer are being used, there is the risk of misappropriating the data from a printer port on the computer entity after it has been decrypted and after it has been checked that the document is intended for the particular computer entity as modified by the application, i.e. a specific recipient device. However, there is still an improvement compared to prior art 30 document transfer systems, because once the document has been sent to print, the electronic version of the document file is deleted from the computer entity.

30

The application can either be embedded with a unique identifier data during manufacture, for which is different for each particular application, or a unique

identifier data can be provided in an external plug in device e.g. dongle (dongle devices being known in the art), where the external device is programmed with the unique identifier data which converts the conventional computer entity into an authorised recipient device.

5

In the implementations described herein, in a best mode the sending computer entity and recipient devices are factory embedded with unique device identifier data which pre-match, and make the sending computer entity and recipient devices difficult to tamper with. In other implementations, the sending 10 computer entity may be allocated a large number of possible unique device identifiers, enabling expansion of the system to incorporate further authorised recipient devices. Each authorised recipient device may be provided at manufacture with the decryption algorithms without embedding the unique device identifier data, and the unique device identifier data may be installed in a recipient 15 device after manufacture, for example in the form of a plug in hardware device e.g. a dongle or similar.

**Claims:**

1. A printer device comprising:

a data input device for receiving an encrypted digital document file;

5

a decryption algorithm for decrypting said received document file;

a controller for controlling printing of an image of data contained in said received document file; and

10

a printer mechanism for printing a physical copy of said document file,

wherein said controller operates to control printing of said physical copy, and after printing of said physical copy, delete said electronic document file from 15 said memory.

2. The printer device as claimed in claim 1, comprising a network interface for receiving said encrypted digital document file over a network.

20

3. The printer device as claimed in any one of the preceding claims, wherein said controller stores a unique device identification data uniquely identifying said printer device, said controller operating to:

25 compare a received unique identifier data contained in said received document file with said stored unique device identifier;

if said received unique device identifier data differs from said stored unique device identifier data, delete said document file.

30

4. The printer device as claimed in any one of claims 1 to 3, wherein said controller stores a unique device identification data uniquely identifying said printer device, said controller operating to:

compare a received unique identifier data contained in said received document file with said stored unique device identifier;

5 if said received document identification data is identical to said received unique device identifier data, control said print mechanism to print at least one said physical copy of said document file.

5. The printer device as claimed in claim 1, wherein:

10 said controller operates to read a quantity permission data content of said document file, said quantity permission data specifying a number of authorised copies of said document file to be printed; and

15 said controller controls said print mechanism such that said permitted quantity of physical copies of said document file are printed.

6. The printer device as claimed in any one of claims 1 to 5, wherein:

20 said controller operates to generate a confirmation message confirming receipt of said document file.

7. The printer device as claimed in claim 6, wherein said confirmation message comprises a time and date data, specifying a time and date of receipt of said document file; and

25 a number of copies printed data, specifying a number of copies of said document file physically printed by said print mechanism.

30 8. A printer device comprising:

a data input device for receiving an encrypted digital document file;

a decryption algorithm for decrypting said received document file;

5        a controller for controlling printing of an image of data contained in said received documents file; and

10        a printer mechanism for printing a physical copy of said document file, wherein said controller operates to check a unique device identification data contained in said document file with a stored unique device identification data of said printer device, and provided a successful match is found, print said physical copy of said document file.

9.        A computer entity configured for sending secure encrypted document files, said computer entity comprising:

15        a data processor;

20        a memory;

25        an encryption algorithm capable of encrypting a document file; a device selector for selecting a said uniquely identifiable recipient device; a file selector for selecting a document file;

30        a stored list of a set of authorised recipient devices, each said recipient device identified by a unique device identifier data inaccessibly embedded within said computer entity; wherein said computer entity operates to: select at least one document file;

select at least one device of said set of uniquely identified recipient devices to send said document to;

5        encrypt said document files; and

address said at least one document file to said selected uniquely identified device(s).

10        10.        The computer entity as claimed in claim 9, further comprising:

a network interface capable of sending said document file over a network to a selected said recipient device.

15        11.        The computer entity as claimed in claim 9, further comprising a user interface capable of displaying a history list of document files sent, said history list comprising:

data describing a document file sent;

20

data describing at least one recipient device to which said document file has been sent;

25        data describing a number of copies of documents said recipient device is authorised to print from said received document file.

12.        The computer entity as claimed in claim 9, wherein said user interface further displays:

30        data describing an encryption method used for sending said document.

13. The computer entity as claimed in claim 9, wherein said user interface displays:

an acknowledgement message data describing receipt of said document file  
5 by a said recipient device.

14. A distributed secure document printing system, said system comprising:

10 at least one sending computer entity, capable of sending an encrypted electronic document file, said document file having an encrypted data content, and a unique device identifier data identifying a recipient device to which said document file is sent: and

15 at least one recipient printer device, said recipient printer device capable of receiving said encrypted document file, establishing that said document file is intended for said recipient device, decrypting and printing said document file, and deleting said electronic document file after printing a physical copy of a document from said document file.

20 15. The system as claimed in claim 14, wherein said recipient printer device is capable of reading a permitted quantity data content of said document file; and

25 printing a number of physical copies of said document file, corresponding to said permitted quantity data.

16. The system as claimed in claim 14 or 15, wherein:

30 said recipient printer device is configured to send a confirmation message back to said sending computer entity, confirming receipt of said document file, and printing of a specified permitted number of copies of said document file.

17. A method of securely communicating an electronic document file over a network, said method comprising the steps of:

5 encrypting said document file;

specifying a recipient device for sending said document file to, said recipient device being uniquely identifiable by a unique device identifier data;

10 attaching said unique identifier data to said document file;

sending said document file in encrypted format to said intended recipient device;

15 receiving said transmitted document file and decrypting said document file;

reading said unique device identifier data;

20 if said unique device identifier data corresponds to a unique device identifier data of said recipient device, printing a physical copy of said document files.

18. The method as claimed in claim 17, further comprising the step of:

25 after printing said physical copy, deleting a said electronic document file from said recipient device.

19. The method as claimed in claim 17, further comprising the step of:

30 specifying a permitted quantity of physical copies of said document file to be printed; and

printing said permitted number of copies of said document file.

20. A method of secure printing of a received document file, said method comprising the steps of:

5 receiving said document file in encrypted format;

decrypting said document file;

10 reading a unique device identifier data identifying a recipient device for which said document file is intended;

15 comparing said unique device identifier data with a locally stored device identifier data;

if said received unique device identifier data corresponds with said locally stored device identifier data, printing a physical copy of said document file.

21. The method as claimed in claim 20, further comprising the step of:

20 deleting said electronic document file, after printing said physical copy of said document file.

22. The method as claimed in claim 20, further comprising the step of:

25 reading a permitted quantity data describing a permitted quantity of copies of said document file; and

printing said permitted quantity of copies of said document file.

30 23. The method as claimed in claim 20, wherein said document file, after decryption is prevented from being viewed on a visual display device prior to printing.

24. The method as claimed in claim 20, wherein said document file is received over a network connection.

5 25. The method as claimed in claim 20, wherein said document file is received via an intermediary carrier device having data storage capability.

26. A method of sending a document file for printing by a specified authorised recipient printing device, said method comprising the steps of:

10 selecting a content of said document file;

encrypting said content;

15 attaching a unique device identifier data, identifying a recipient device to which said document file is to be sent; and

sending said document file to said recipient device.

20 27. The method as claimed in claim 26, further comprising the step of:

adding a permitted quantity data to said document file, said permitted quantity data specifying a permitted number of copies of said document file which can be printed.

25

28. The method as claim in claim 26, further comprising the step of:

storing a document history data, said document history data specifying for said document file:

30

a list of recipient device(s) to which said document file may be sent;

a number of permitted copies of said document file which are permitted to be printed by each of said recipient device(s).

29. A computer entity comprising a data processor, a data storage device, a printer port, and having an attached printer device, said computer entity comprising:

10 a module for decrypting an encrypted document file;  
a unique device identifier to identify said computer entity into a uniquely;

wherein said computer entity operates to:

15 receive a document file in encrypted format;  
decrypt said document;

20 extract a unique device identifier data from said document and compare said extracted unique identifier data with said unique device identifier of said computer entity;

25 if a match is found between said received unique device identifier data and said unique identifier of said computer entity, send a said document file for print by said printer device; and

after sending said document to said printer device, delete said document file.



Application No: GB 0102428.0  
Claims searched: 1-8, 14-16 & 17-29

Examiner: Catherine Allen  
Date of search: 27 November 2001

## Patents Act 1977

### Search Report under Section 17

#### Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): G4A: AAP

Int Cl (Ed.7): G06F 1/00, 3/12, 12/14

Other: Online: WPI, EPODOC, JAPIO, INSPEC

#### Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	EP1091275	CANON KK	1
X	EP0935182	HEWLETT PACKARD	1, 2 & 5-7
X	EP0929023	HEWLETT PACKARD	1, 2 & 5-7
X	WO98/07254	GALBRAITH et al	1, 2 & 5-7

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.